

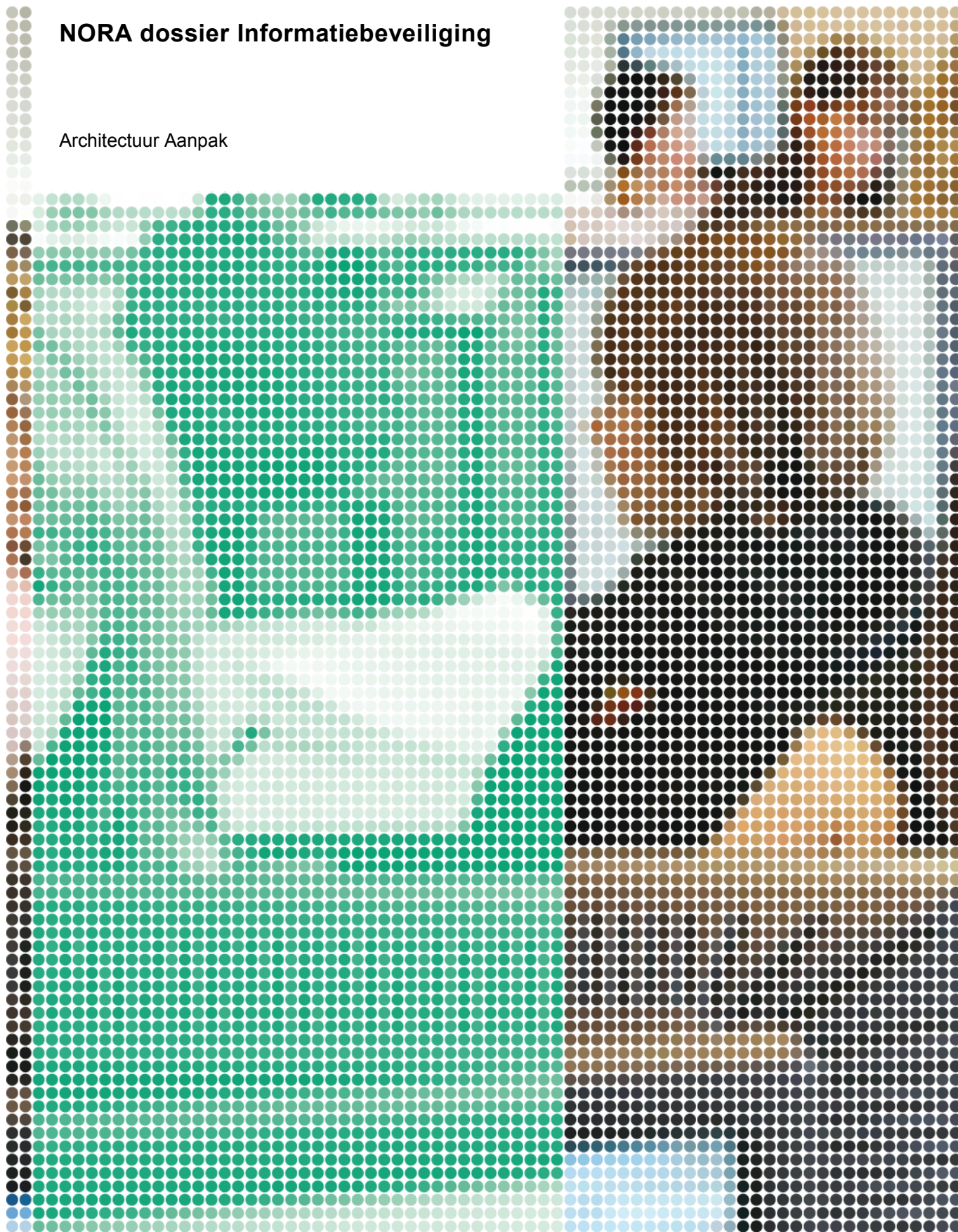


e^overheid

BOUW MEE AAN BETERE DIENSTVERLENING

NORA dossier Informatiebeveiliging

Architectuur Aanpak





e-overheid

BOUW MEE AAN BETERE DIENSTVERLENING

NORA dossier Informatiebeveiliging

Architectuur Aanpak

.....

Auteur	Jaap van der Veen en Bart Bokhorst; Belastingdienst
Versie	1.3
Status	Definitief
Den Haag,	01-09-2010

Inhoud

1	Inleiding	4
2	Modelleringsaanpak	5
3	Model IB-functies	7
4	Beschouwingsmodel	9
5	Overzichtsmodel-IB	10
6	IB-patronen	12
7	Template van een IB-patroon	13

Figuur 1 NORA aanpak architectuur IB	5
Figuur 2 Model IB-functies	7
Figuur 3 Beschouwingsmodel van een NORA keten	9
Figuur 4 Overzichtsmodel voor Integriteit en vertrouwelijkheid van een NORA keten	10
Figuur 5 Overzichtsmodel voor controleerbaarheid van een NORA-keten	11
Figuur 6 Voorbeeld context	13
Figuur 7 Voorbeeld oplossing	13

1 Inleiding

NORA

Burgers en bedrijven verwachten een goed functionerende, dienstverlenende overheid. Samenwerking tussen overheidsorganisaties is hiervoor een belangrijke voorwaarde. Daarbij stemmen zij processen af en maken gebruik van elkaars informatie. NORA, de Nederlandse Overheid Referentie Architectuur, helpt de samenwerking te realiseren.

Voor de NORA heeft een expertgroep Informatiebeveiliging beveiligingsprincipes uitgewerkt in een in een afzonderlijk katern. Uiteindelijk zijn deze principes als algemene kwaliteitsprincipes in NORA 3.0 opgenomen. Onder auspiciën van deze expertgroep hebben de auteurs (zie Colofon) een best practice ontwikkeld, die tevens is meegenomen in de openbare review van genoemd katern in de zomer van 2009. Op grond van de ontvangen commentaren zijn veel verbeteringen aangebracht.

Deze best practice wordt onder de eigen verantwoordelijkheid van de NORA-expertgroep Informatiebeveiliging uitgebracht en heeft daarmee geen andere status dan een advies aan de gebruikers van de NORA hoe de afgeleide kwaliteitsprincipes kunnen worden geïmplementeerd. De expertgroep is inmiddels opgeheven. Deze best practice wordt verder onderhouden door de community van het Platform voor Informatiebeveiliging (PvIB), die zich bezighoudt met het ontwikkelen van beveiligingspatronen, zie <http://www.ibpedia.nl/>, zoek op "IB-patronen".

Architectuur aanpak Informatiebeveiliging

Deze best practice beschrijft de aanpak waarmee invulling kan worden gegeven aan het analyseren, adviseren en toetsen van informatiebeveiligingsaspecten in architectuurmodellen. In deze aanpak wordt een verbinding gelegd tussen architectuurmodellen en een standaard model voor IB-functies met het daarbij behorende normenkader, zie NORA best practice: Normen Informatiebeveiliging IT-voorzieningen.

Architectuurmodellen voor informatiebeveiliging richten zich meestal op de IT-oplossingen, die in een organisatie worden gekozen voor beveiligingsfuncties. In de NORA-benadering wordt uitgegaan van informatiebeveiliging als *kwaliteitsaspect*.

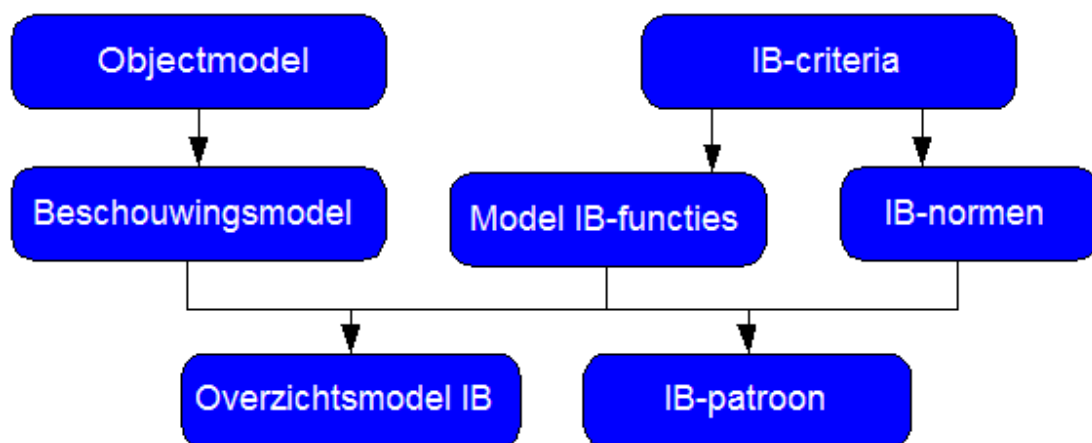
Deze NORA architectuuraanpak wordt verder uitgebouwd en geconcretiseerd met IB-patronen, die als architectuurmodules kunnen worden gezien. De patronen volgen de abstractieniveaus van de NORA best practice: Normen Informatiebeveiliging IT-voorzieningen.

Doelgroep

De doelgroep van de IB-architectuur is de architect, ontwerper, IB-specialist en IT-auditor. Die kunnen de modellen gebruiken als gereedschap voor het maken van IT-ontwerpen voor informatiebeveiliging, het adviseren over het treffen van beveiligingsmaatregelen of het toetsen van ontwerpen aan normen.

2 Modelleringsaanpak

Voordat de verschillende stappen in de modelleringsaanpak worden uitgelegd, geeft Figuur 1 een overzicht van deze stappen.



Figuur 1 NORA aanpak architectuur IB

Informatiebeveiliging beschouwen wij als een kwaliteitsaspect van de bedrijfsvoering van een organisatie. Dat betekent dat we eerst iets over die bedrijfsvoering moeten weten om vandaar uit naar informatiebeveiliging te kunnen kijken. De bedrijfsvoering wordt in architectuurplaten meestal afgebeeld in een z.g. *objectmodel* met bedrijfsfuncties, objecten en interacties.

Omdat beveiliging als *aspect* geheel verweven is in de architectuur van de bedrijfsvoering en kwaliteitsaspecten niet als bedrijfsfuncties kunnen worden afgebeeld, hebben we een aparte plaat nodig om duidelijk te maken waar beveiligingsfuncties in een architectuur werkzaam moeten zijn.

Beveiliging komt in IT-ontwerpen voor als afzonderlijk herkenbare objecten, zoals bijvoorbeeld firewalls en toegangsmoedules maar ook in niet direct herkenbare gedaantes, zoals parameters in een besturingssysteem of een functiescheiding. Om de beveiligingsobjecten en functies in een architectuur af te kunnen beelden, gebruiken we de architectuurplaat: *beschouwingsmodel*.

In het beschouwingsmodel tekenen we vervolgens de IB-functies met hun onderlinge relaties, waaruit een architectuurplaat ontstaat voor Informatiebeveiliging. Deze plaat noemen we het *overzichtsmodel-IB*.

Omdat de compartimentering (zonering) van netwerken en de positionering van IT-systemen daarin in belangrijke mate bepaald wordt door beveiliging, kiezen we er voor om de architectuurplaten daarmee vorm te geven. Voor inzicht in details van de oplossingen worden IB-patronen gebruikt.

Samengevat omvat in deze aanpak van een IB-architectuur dus een model of een reeks van modellen, dat laat zien hoe het bedrijfsfuncties samenhangen met het kwaliteitsaspect Informatiebeveiliging.

Een IB-patroon, als onderdeel van de IB-architectuur is een standaard beschrijving van een probleem en oplossing binnen een bepaalde context, met als doel dat de oplossing algemener inzetbaar wordt. Patronen zijn te beschouwen als *bouwstenen* op architectuurniveau.

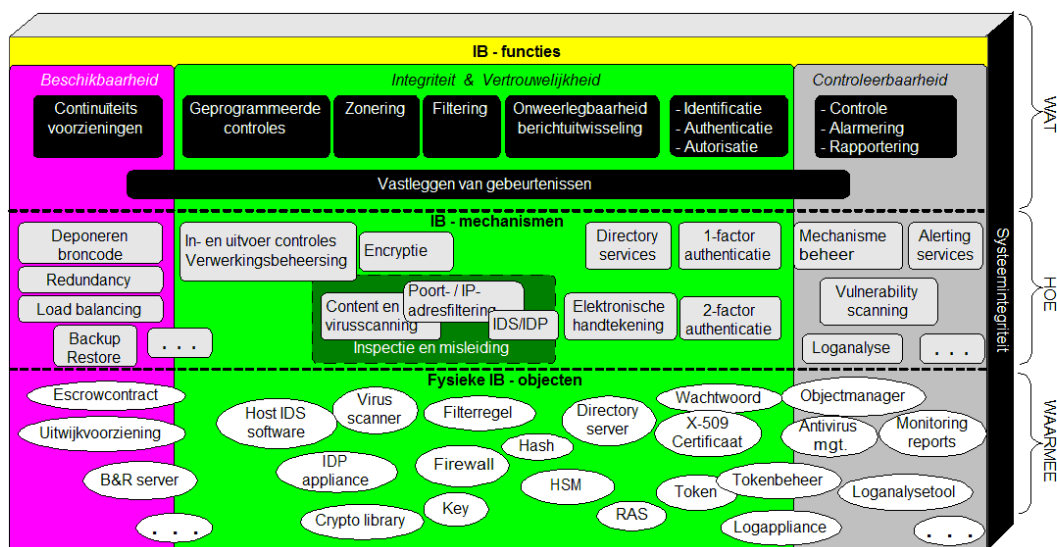
De hier geschetste architectuuraanpak wordt momenteel door een community van de PvIB verder uitgebouwd door het modelleren van veel voorkomende beveiligingssituaties in IB-patronen. De focus van de IB-patronen is daarbij vooralsnog gericht op IT.

3 Model IB-functies

Het referentiekader voor de modelleringaanpak wordt gevormd door het model IB-functies van Figuur 2, dat bedoeld is om te ordenen en te verbinden. Het model is een NORA-doorontwikkeling van ISO-NEN 7498-2¹

Een IB-functie is een logische groepering van geautomatiseerde activiteiten, die op een bepaald beveiligingsdoel is gericht. In samenhang worden de negen afgebeelde beveiligingsfuncties dekkend geacht voor de informatiebeveiliging van IT voorzieningen (zwarte functieblokken).

In het architectuurmodel zijn deze IB-functies geprojecteerd op de kwaliteitscriteria voor informatiebeveiliging: Beschikbaarheid, Integriteit, Vertrouwelijkheid en Controleerbaarheid. In *samenhang* vormen ze de WAT-laag van het model.



Figuur 2 Model IB-functies

De IB-functies met bijbehorende mechanismen en fysieke objecten, zijn voor de eenvoud van afbeelding, op de criteria geprojecteerd, die ze *primair* ondersteunen, maar de functies voor integriteit en vertrouwelijkheid dragen bijvoorbeeld ook bij aan beschikbaarheid. Per IB-functie wordt een doelstelling, definitie, toelichting en motivering gegeven in de NORA best practice Normen informatiebeveiliging IT-voorzieningen.

¹ISO-NEN 7498-2[1] Information processing systems : Open Systems Interconnection Basic Reference Model – Part 2: Security Architecture uit 1991.

.....

De IB-mechanismen vormen de HOE-laag en zijn *technische* concepten (technieken) die het WAT van de IB-functies invullen. Omdat techniek zich steeds verder ontwikkelt, illustreert de figuur slechts een aantal bekende voorbeelden.

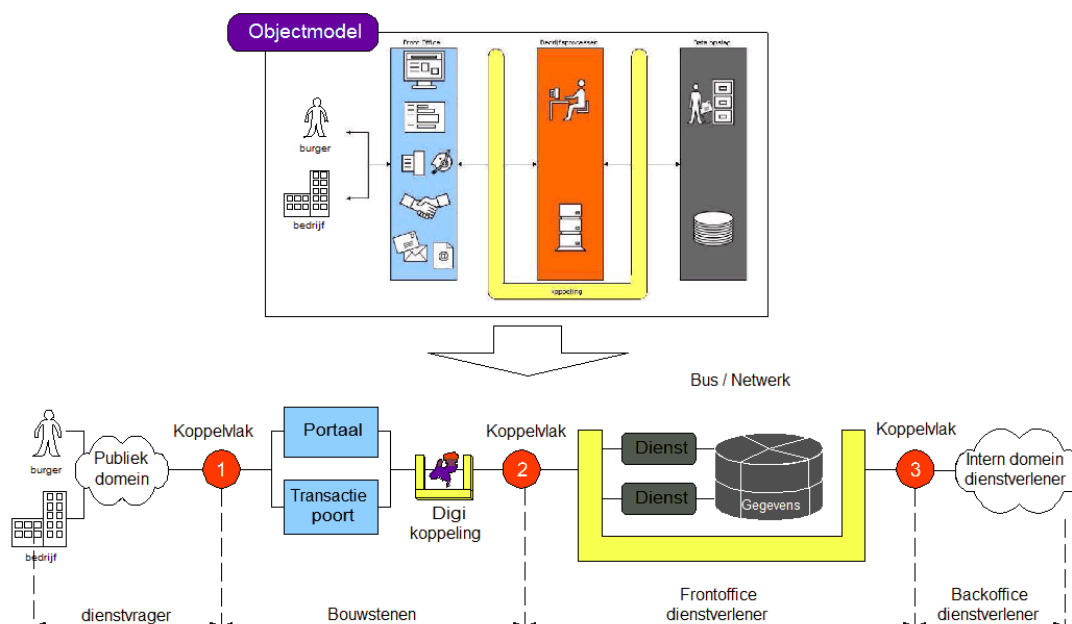
De fysieke IB-objecten vormen de WAARMEE-laag. Dit zijn IT-onderdelen, die de IB-mechanismen daadwerkelijk uitvoeren. Ze kunnen onderdeel zijn van een besturingsprogramma of applicatie, maar worden ook als afzonderlijke fysieke modules uitgevoerd. Ook hier zijn slechts enkele bekende voorbeelden getekend. Hoewel referentiearchitecturen de HOE- en WAARMEE-laag meestal niet beschrijven, is dat hier wel gedaan om duidelijk te maken hoe en waarmee beveiligingsfuncties uiteindelijk werkzaam kunnen zijn in de IT.

In de beschrijving die nu volgt is aangegeven welke modellen we gebruiken om informatiebeveiliging in een ontwerp inzichtelijk te maken.

4 Beschouwingsmodel

Het beschouwingsmodel is een vertaling van het objectmodel, die we gebruiken om de relatie met IB-functies aan te geven. Figuur 3 geeft aan hoe een beschouwingsmodel van bijvoorbeeld een NORA-keten er uit kan zien waarbij de “Basisarchitectuur overheidsorganisatie” als objectmodel dient.

De vertaalslag bestaat eruit dat alleen IT-voorzieningen in beschouwing worden genomen en dat er koppelvlakken worden gebruikt om netwerkzones zichtbaar te maken. De koppelvlakken zijn genummerd om ze afzonderlijk voor beveiliging te kunnen beschouwen.



Figuur 3 Beschouwingsmodel van een NORA keten

Als toelichting op het NORA voorbeeld nog het volgende:

De IT-voorzieningen *Portaal* en *Transactiepoort* die centraal voor de overheid als frontoffice dienen, zijn in een afzonderlijke netwerkzone opgenomen onder de term *Bouwstenen*, omdat ze in de NORA zo worden aangeduid.

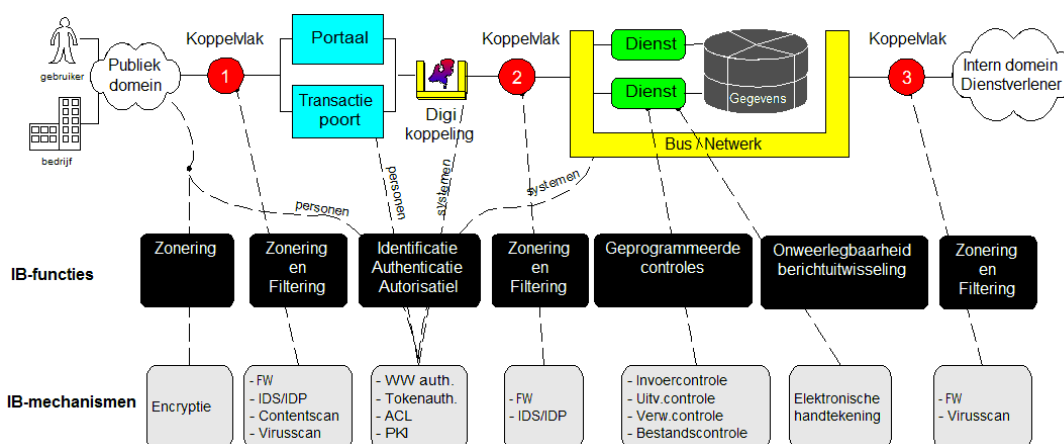
Ook *Digikoppeling*, als een reeks standaarden voor het uitwisselen van elektronische gegevens binnen de overheid is zo'n bouwsteen.

Met *dienstverlener* wordt de desbetreffende overheidsinstantie bedoeld, die informatie wil uitwisselen met burgers en bedrijven.

5 Overzichtsmodel-IB

Het overzichtsmodel ontstaat door op het beschouwingsmodel de relevante IB-functies af te beelden met de bijbehorende IB-mechanismen. De daarmee verkregen schets van functies en uitvoerende mechanismen is hier als voorbeeld niet uitputtend, maar dient voor het verkrijgen van overzicht en inzicht in de plek waar IB werkzaam is in bedrijfsketens en infrastructuur.

Voor de eenvoud beperken we de scope van het overzichtsmodel bijvoorbeeld tot het afbeelden van de vereiste Integriteit en Vertrouwelijkheid voor een bepaalde infrastructuur, of alleen voor het criterium Controleerbaarheid. Op dit globale niveau worden de fysieke IB-objecten weggelaten. De IB-functie continuïteitsvoorzieningen blijkt in de praktijk niet eenvoudig te kunnen worden afgebeeld in overzichtsmodellen. Daarvoor is een gedetailleerder en meer fysiek georiënteerd model nodig, zoals een configuratieschema.

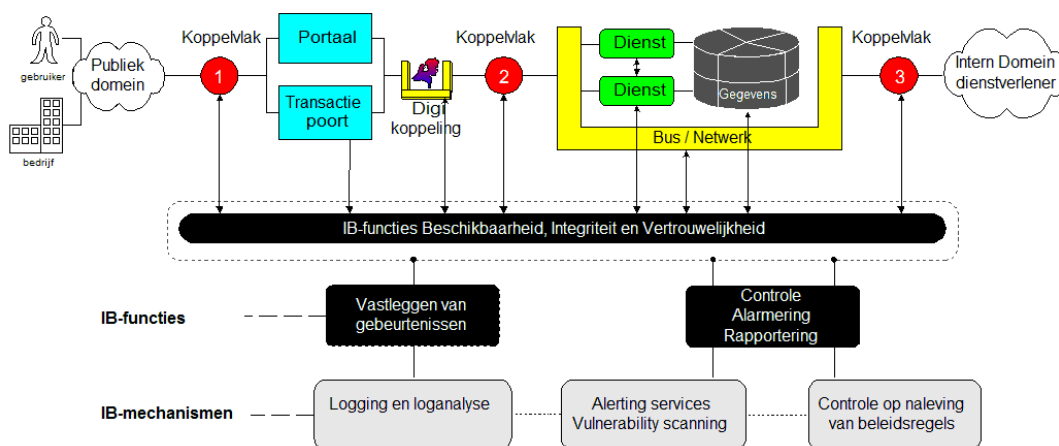


Figuur 4 Overzichtsmodel voor Integriteit en vertrouwelijkheid van een NORA keten

Als voorbeeld van een overzichtsmodel laat Figuur 4 zien hoe de IB-functies voor de criteria Integriteit en Vertrouwelijkheid in een NORA-keten uitwerken. Voor betrouwbare communicatie tussen burger en overheid is een vertrouwd toegangspad gewenst tot het portaal van de overheid. Daarvoor is encryptie gebruikt.

Vanaf het portaal tot aan het interne domein van de ketenpartner is er sprake van een besloten netwerk. Ook dit kan als een vertrouwd toegangspad worden beschouwd, mede door de werking van de andere in dit pad gepositioneerde IB-functies. Merk op dat de functies Zonering en Filtering op verschillende plaatsen in de keten door IB-mechanismen op een andere manier wordt ingevuld. De positionering van geprogrammeerde controles kan in dergelijke globale modellen uiteraard maar beperkt zichtbaar worden gemaakt als gevolg van de verwevenheid daarvan met applicaties (hier Dienst genoemd). Dit geldt in zekere zin ook voor alle andere mechanismen.

De zeggingskracht van deze overzichtsmodellen zit met name niet in de *volledigheid* van het afbeelden van beveiligingsmaatregelen, maar veel meer in het *totale* en (dus) *globale* inzicht. Voor een meer gedetailleerd inzicht kunnen onder meer de IB-patronen worden gebruikt.



Figuur 5 Overzichtsmodel voor controleerbaarheid van een NORA-keten

Figuur 5 laat zien welke IB-functies voor Controleerbaarheid werkzaam zijn in een NORA-keten. IB-mechanismen voor integriteit en vertrouwelijkheid worden ingesteld en beheerd door afzonderlijke tools of met tooling die in de IT-voorzieningen zelf is geïntegreerd.

Beveiligingsgebeurtenissen die in de IT-keten hebben plaatsgevonden, worden vastgelegd voor controledoeleinden. Dit vastleggen (loggen) vereist aparte infrastructurele voorzieningen. Wanneer drempelwaarden worden overschreden van bijvoorbeeld een firewall, IDS of virusscanner, dan moet een mechanisme zorgdragen voor alarmering naar een systeembeheerder of een CERT[1].

Evenals geldt voor de criteria Integriteit en Vertrouwelijkheid, worden voor Controleerbaarheid door de keten heen steeds dezelfde functies toegepast, maar de toegepaste mechanismen en objecten kunnen per situatie verschillen.

6 IB-patronen

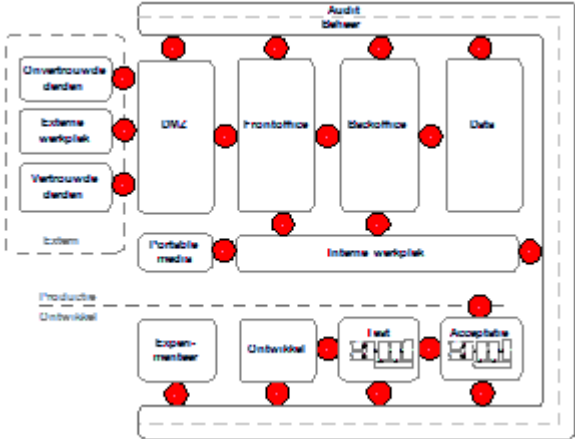
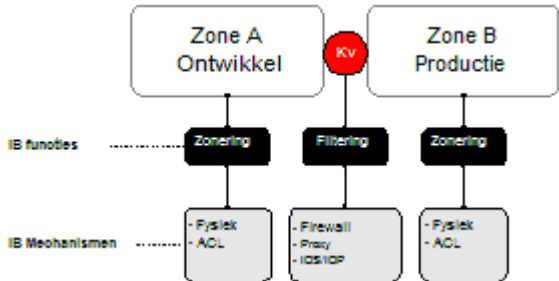
Een patroon is een abstractie van een probleem en oplossing binnen een bepaalde context, met als doel de oplossing algemener inzetbaar te maken. Patronen zijn vooral bedoeld als *middel* om oplossingen op een compacte standaard manier te beschrijven en die oplossingen daarmee toegankelijk te maken.

De Open Group heeft voor patronen een beschrijvingsmodel ontwikkeld die voor de IB-patronen zijn aangevuld met enkele extra rubrieken om beter praktisch bruikbaar te maken, zie de Template.

IB-patronen kunnen zowel thematisch als hiërarchisch worden gerubriceerd. We onderkennen daarbij patronen die een oplossing bieden voor één specifiek probleem (b.v. Digitale Handtekening), maar ook patronen die een bepaald thema beschrijven, zoals b.v. koppelvlakken en Identity & Access Management (IAM). Elk thema kan daarbij bestaan uit verschillende specifieke patronen.

In de vakliteratuur (o.a. de Open Group) zijn patroonbeschrijvingen ("security patterns") beschikbaar. Deze worden in de praktijk echter weinig gebruikt omdat ze in de academische wereld zijn ontstaan en blijven hangen in een (te) hoog abstractieniveau. De hier bedoelde IB-patronen worden in de community van het PvlB door beroepsgenoten ontwikkeld vanuit de praktijk. Daarnaast wordt in de patronen de link gelegd naar normen voor informatiebeveiliging.

7 Template van een IB-patroon

Rubriek	Omschrijving
	<p>Naam</p> <p>Vat het doel van het patroon kort samen, bij voorkeur in termen van de oplossing</p>
Criteria	Welke van de IB-criteria: <i>Beschikbaarheid</i> , <i>Integriteit</i> , <i>Vertrouwelijkheid</i> en <i>Controleerbaarheid</i> zijn aan de orde?
Context	<p>Hoe ziet de omgeving er uit waarin het probleem zich voordoet, bij voorkeur te benaderen aan de hand van de standaard context: het patroon Zonering</p>  <p>Figuur 6 Voorbeeld context</p>
Probleem	Welk risico moet worden beheerst?
Oplossing	<p>Welke (technische) beveiligingsmaatregelen zijn er als (standaard) oplossing te geven?</p>  <p>Figuur 7 Voorbeeld oplossing</p>
Afwegingen	Wat zijn de voor- en nadelen en doorslaggevende argumenten voor de keuze van de oplossing?
Voorbeelden	Welke beproefde toepassingsvoorbeelden van de oplossing zijn er te geven?

.....

Implicaties	<p>Wat moet de organisatie doen om gebruik te kunnen maken van de geboden oplossing van een patroon? (impact en randvoorwaarden)</p> <p>Wat zijn de gedragskenmerken tijdens operationeel gebruik?</p>		
Gerelateerde patronen	Van welke patronen is de oplossing (van dit patroon) afhankelijk?		
Normen	Aan welke Beheersmaatregelen dan wel Implementatierichtlijnen van NORA Best practice Normen Informatiebeveiliging IT-voorzieningen geeft dit patroon invulling?		
	IB functie	Beheersmaatregel	Implementatierichtlijnen
	5. Zonering	5.1 Zonering technische infrastructuur	1. Er zijn aparte zones voor Ontwikkeling, Test, Acceptatie en Productie (bijvoorbeeld)
	6. Filtering	6.1 Controle op communicatiegedrag	3. Al het gegevensverkeer vanuit externe of onvertrouwde zones wordt real-time inhoudelijk geïnspecteerd op inbraakpogingen. (bijvoorbeeld)

.....

Colofon

Versie : 1.3
Datum : 01-09-2010
Status : Definitief
Expertgroep : Informatiebeveiliging
Auteurs : Jaap van der Veen en Bart Bokhorst; Belastingdienst
Contactadres : architectuur@e-overheid.nl
Licentie : Dit document is beschikbaar onder de volgende Creative Commons
licentie: <http://creativecommons.org/licenses/by-nd/3.0/nl/>

Wilhelmina van Pruisenweg 104
2595 AN Den haag
Postbus 84011
2508 AA Den Haag

T (070) 888 78 20
F (070) 888 78 81
www.e-overheid.nl

